

- Hardware Security Module



SRJ1511

e-Signature & Verification HSM

Product Functions

Algorithm Support

- SM1 / SM2 / SM3 / SM4
- DES / 3DES / AES / IDEA / RSA
- SHA* / MD5

Technical Support

- SM2 and RSA algorithms to provide signature verification for data, messages and files
- Support P1 and P7 format including attached signature and detached signature, and PKCS1# naked sign
- IP address filtering function (whitelist) by managing access to the equipment from client
- Log auditing including transaction logs and management logs
- Application entity information registration, key authorization configuration, setting private key authorization code
- Certificate related functions: issuing authority certificate, application entity certificate, user certificate, etc. certificate application message generation, import, deletion, certificate validity verification, etc.
- Digital envelope generation and decryption in P7 mode
- Support XML digital signature and verification
- True random number generation

Product Features

High Compatibility

- Full range of algorithms
- Complete functional interfaces
- Compatible with the mainstream key system

Reliability

- The hardware and software architectures adopt redundancy design
- Support cluster management
- MTBF = 30,000 hours

Superior Performance

- The maximum value of symmetric algorithm =40,000TPS
- The maximum value of asymmetric algorithm=50,000TPS

Efficiency

- Providing multi-channel secure management modes (native management & remote management)

Security

- Secure and reliable key protection mechanism to support the emergency destruction mechanism
- Monitoring equipment status and providing API access to customers' internal monitoring system

Successful Cases

